



Habtamu Abie, Davide Ferrario, Ernesto Troiano,  
John Soldatos, Fabrizio Di Peppo, Aleksandar Jovanović,  
Ilias Gkotsis, Evangelos Markakis (Eds.)

# Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection

Virtual Workshop, June 24–25, 2020

# **Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection**

Virtual Workshop, June 24–25, 2020

Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo,  
Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Eds.)



**Steinbeis-Edition**

# Abstract

Modern critical infrastructures (“critical entities” in the terminology of the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. To face them successfully, aligned and integrated responses are needed, and this workshop has provided a great opportunity to do it: aligning and integrating not only the positions of single projects but also of many intended users of their results.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in seven different industrial sectors, such as finance, healthcare, energy, air transport, communications, industrial plants, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.

Specifically, novel techniques have been presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, resilience of critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures.

The workshop included two opening remarks, two keynote speeches, 11 project presentations, 2 roundtable and panel discussions and 10 thematic presentations. The audience included scientists and experts in the field of critical infrastructure protection, CISOs, CIOs, CERTs, CSIRTs, CSOs, cyber and physical security experts representing different sector and policy makers for Critical Infrastructure protection.

# Table of Contents

1. Organizations .....	6
2. Program Agenda .....	6
3. Welcome and Opening Remarks.....	9
3.1 Opening Remarks.....	9
3.2 The ECSCI Cluster Achievements .....	9
3.3 Critical Infrastructure Protection: Main messages .....	13
4. Keynotes.....	14
4.1 Critical Information Infrastructure Protection: The role of ENISA in the new EU policy context.....	14
4.2 Moving towards a trustworthy and resilient European cyber security ecosystem .....	14
5. Project Presentations.....	15
5.1 Security and trust assessment in CPS / IOT architectures .....	15
5.2 Energy infrastructure protection .....	17
5.3 Securing critical financial infrastructure .....	18
5.4 Improving resilience of sensitive industrial plants and infrastructures.....	20
5.5 Resilience enhancement and risk control for communication infrastructures .....	21
5.6 Safeguarding critical health infrastructure .....	23
5.7 Security of air transport infrastructure of Europe.....	25
5.8 Securing the European gas network .....	27
5.9 Resilience of Smart Critical Infrastructures .....	27
5.10 Cyber-security protection in healthcare IT ecosystem .....	29
5.11 Protection of critical water infrastructures .....	30
6. Round tables and Panel Discussions .....	33
6.1 Artificial Intelligence .....	33
6.2 ELSI – Ethical, legal, and social implications of project.....	33
7. Thematic Presentations .....	35
7.1 Physical and Cyber security integration and modelling.....	35
7.1.1 Applied to WATER critical infrastructure .....	35
7.1.2 FINSTIX Data Modelling for Financial Critical Infrastructures.....	37
7.1.3 SAFECARE approach to integrated cyber-physical security for the healthcare sector .....	38
7.2 Standardization in Critical Infrastructure Protection.....	39
7.3 Collaborative Risk Assessment.....	40
7.4 Protect Industry 4.0 .....	41
7.5 Cyber and Physical Security management.....	42
7.6 Resilience of Critical Infrastructures .....	43
7.7 Increased Automation .....	43

7.8	Legal and Ethical issues.....	43
7.8.1	Introduction .....	44
7.8.2	Context.....	44
7.8.3	Setting the framework .....	44
7.8.4	Regulatory challenges and opportunities for the CIP in healthcare: the ECI Directive 45	
7.8.5	Regulatory challenges and opportunities for CIIP in healthcare: the NIS Directive .....	45
7.8.6	Conclusions .....	46
7.9	Predictive Analytics .....	46
7.10	Anomaly detection.....	48
8.	Concluding Remarks and Planning.....	49
8.1	Day 1 and Day 2 .....	49
8.2	Closing Remarks .....	50
8.3	Concluding Remarks.....	50
	Acknowledgements.....	51
	References .....	52

## Imprint

2021 Steinbeis-Edition



Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo,  
Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Eds.)

Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection  
Virtual Workshop, June 24–25, 2020

1st edition, 2021 | Steinbeis-Edition, Stuttgart  
ISBN 978-3-95663-087-3

Layout: Steinbeis-Edition  
Cover picture: Macrovector/shutterstock.com

The platform provided by Steinbeis makes us a reliable partner for company startups and projects. We provide support to people and organizations, not only in science and academia, but also in business. Our aim is to leverage the know-how derived from research, development, consulting, and training projects and to transfer this knowledge into application – with a clear focus on entrepreneurial practice. Over 2,000 business enterprises have already been founded on the back of the Steinbeis platform. The outcome? A network spanning over 6,000 experts in approximately 1,100 business enterprises – working on projects with more than 10,000 clients every year. Our network provides professional support to enterprises and employees in acquiring competence, thus securing success in the face of competition. Steinbeis-Edition publishes selected works mirroring the scope of the Steinbeis Network expertise.

218957-2021-10 | [www.steinbeis-edition.de](http://www.steinbeis-edition.de)

Modern critical infrastructures ("critical entities" in the terminology of the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. To face them successfully, aligned and integrated responses are needed, and this workshop has provided a great opportunity to do it: aligning and integrating not only the positions of single projects but also of many intended users of their results.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in seven different industrial sectors, such as finance, healthcare, energy, air transport, communications, industrial plants, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.

Specifically, novel techniques have been presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, resilience of critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures. The workshop included two opening remarks, two keynote speeches, 11 project presentations, 2 roundtable and panel discussions and 10 thematic presentations. The audience included scientists and experts in the field of critical infrastructure protection, CISOs, CIOs, CERTs, CSIRTs, CSOs, cyber and physical security experts representing different sector and policy makers for Critical Infrastructure protection.